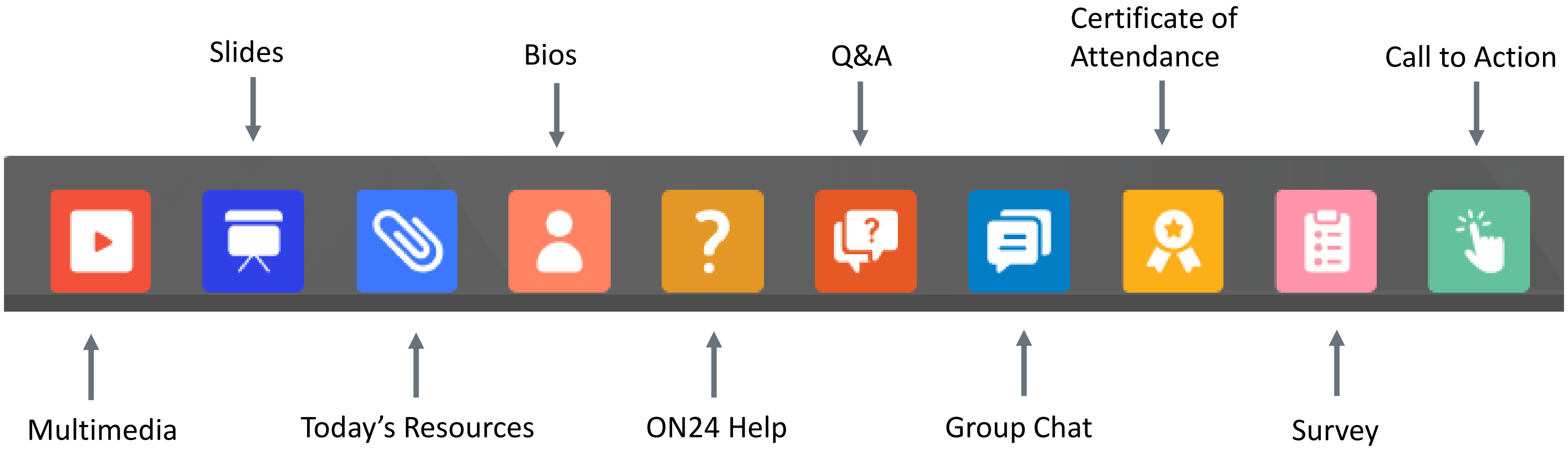
CompTIA Network+ N10-009 TTT Session 9:

Title

July 23, 2024

@TeachCompTIA #NetworkPlusTTT



Slides

Bios

Q&A

Certificate of Attendance

Call to Action

Multimedia

Today’s Resources

ON24 Help

Group Chat

Survey

Network+ Team

Instructor:
Don Tilley
Cybersecurity Instructor,
Program Director
Access Computer Training
dontilley130@gmail.com

Host:
Stephen Schneiter
Instructor Network Program Director
CompTIA
sschneiter@comptia.org

CIN

CompTIA

INSTRUCTOR NETWORK

The CompTIA Instructor Network (CIN) is a worldwide community for instructors who provide CompTIA certification training.

Benefits of being a community member include:

- Communicate and collaborate with CompTIA staff and other instructors.
- Access resources for students to understand the value of getting certified.
- Receive complimentary training and tools from CompTIA to enrich your classroom.
- Become proficient at teaching CompTIA standards.
- Share best practices and resources with each other.

Google Play App Store

https://cin.comptia.org

PARTNERSUMMIT 24

JULY 30TH

CompTIA INSTRUCTOR NETWORK

TRAIN THE TRAINER

WORKSHOPS

CompTIA Network+

CompTIA Tech+

CompTIA A+

Join us for the morning session from 9:00 a.m. to 12:00 p.m. or
the afternoon session from 1:00 p.m. to 4:00 p.m.
Each session is $99.00.
Lunch and refreshments provided

Workshop sessions:

1. Get In Sync with the new CompTIA Tech+ FC0-U71
2. Teaching CompTIA Network+ N10-009 with the new CertMaster Perform
3. Tools for teaching CompTIA A+ 1100 Series

Each session provides:

- Access to official CompTIA content for the course
- Instructor led training and labs
- Certificate of completion provided at the end of session.

Hyatt Regency Atlanta
July 31 – August 1
Register today: https://connect.comptia.org/partnersummit/home

If a bad organizational culture eats ethics for breakfast, then will AI steal your lunch money?

What: One-hour webinar investigating current industry AI trends
When: Thursday July 25th 10:00 a.m. CST
Where: ON24
Who: James Stanger, Chief Technology Evangelist
Register: https://bit.ly/CINPulse-AITrends

@TeachCompTIA

CompTIA

TRAIN THE TRAINER

WEBINAR

COMING SOON

STAY TUNED!

CompTIA

DataX

Complimentary Webinar Series for Instructors

What: 10-session webinar series

When: Aug 12 – Sept 11, 2024

Where: ON24

The CompTIA DataX DY0-001 TTT series will cover:

- DataX exam domains
- Comprehensive understanding of key data science concepts
- Hands-on experience with key technology tools used by data science professionals
- Instructional strategy to implement a DataX course
- Preparation for DataX DY0-001 certification

CompTIA

Network+ N10-009 TTT Session Outline	
Date	Topic
✓ 06/20/2024	Introduction and Network Topologies
✓ 06/25/2024	Cabling and Physical Installations
✓ 06/27/2024	Configuring Interfaces and Switches
✓ 07/02/2024	Configuring Network Addressing
✓ 07/09/2024	Configuring Routing and Advanced Switching
✓ 07/11/2024	Network Security
✓ 07/16/2024	Network Security (Continued)
✓ 07/18/2024	Wireless Networking
✓ 07/23/2024	Troubleshooting and Management
07/25/2024	Emerging Technologies and Trends

SUPPORTING MANAGEMENT NETWORK

Learning Objectives

- Explain the use of configuration and change management documentation.
- Use discovery and monitoring tools to identify network assets.
- Use event management to ensure network availability.
- Use packet analysis and traffic metrics to troubleshoot performance issues.

ORGANIZATIONAL POLICIES AND DOCUMENTATION

Policies and Documentation

Importance of documentation

- Facilitates troubleshooting
- Ensures consistency
- Supports scalability and upgrades
- Supports staff overturn

Types of documentation

- Configuration management
- Backup management
- Change management
- Asset management
- Network management

Configuration Management

✓ Identify service assets

Consider a CMS solution

Determine an identification strategy

Establish a CI management plan

Monitor configuration drift

Network Device Backup Management

- Document backups and procedures
- Maintain a regular backup schedule
- Audit and verify backups
- Maintain version history
- Configure remote logging of state data

Change Management

- Establish a comprehensive documentation protocol
- Ensure consistent use of templates
- Implement version control and access management
- Incorporate a feedback loop
- Regularly review and update documentation

Asset Management - Inventory

Update inventory documentation regularly

Record asset description, purchase date, service history, status, and location

Adopt asset management software tools

Implement strict access controls to inventory documentation

Network Management

Physical network diagrams

- Detail hardware components
- Record location information
- Specify cabling details

Logical network diagrams

- Display protocols being used
- Organize by function vs physical location
- Identify interconnection points

IP address management

- Use a consistent addressing scheme
- Record IP addresses
- Use automation tools

Activity: Worst Case Scenario

What if there wasn’t documentation and….

- The network administrator left the company?
- There was a natural disaster?
- Primary systems crashed?

Poll Questions

What are the key components of an effective configuration management system for network devices?

How does change management documentation contribute to maintaining network stability and security?

Game: "Documentation Puzzle" Match the following terms with their descriptions:

1. Configuration Management
2. Change Management
3. Asset Management
4. Network Diagram

- A. Keeps track of all network equipment and their details B. Shows how network devices are connected and organized C. Ensures network device settings are properly recorded and maintained D. Controls and documents changes made to the network

HOST DISCOVERY & MONITORING

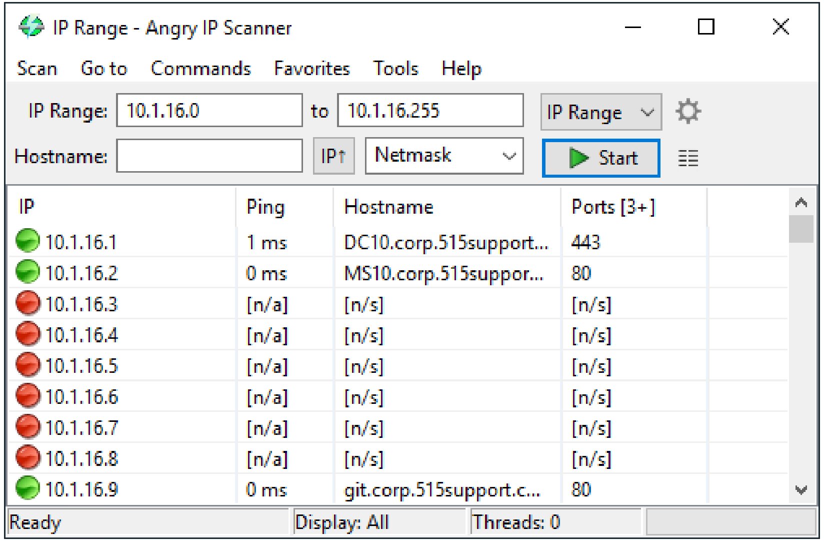
Network Discovery

Network Discovery

- Identifying network devices and services
- Network management and security auditing

Network Discovery Tools

- Nmap
- AngryIP
- PRTG



IP Range - Angry IP Scanner
Scan Go to Commands Favorites Tools Help
Start

IP Range: 10.1.16.0 to 10.1.16.255 IP Range

Hostname: IP↑ Netmask

IP	Ping	Hostname	Ports [3+]
🟢 10.1.16.1	1 ms	DC10.corp.515support...	443
🟢 10.1.16.2	0 ms	MS10.corp.515suppor...	80
🔴 10.1.16.3	[n/a]	[n/s]	[n/s]
🔴 10.1.16.4	[n/a]	[n/s]	[n/s]
🔴 10.1.16.5	[n/a]	[n/s]	[n/s]
🔴 10.1.16.6	[n/a]	[n/s]	[n/s]
🔴 10.1.16.7	[n/a]	[n/s]	[n/s]
🔴 10.1.16.8	[n/a]	[n/s]	[n/s]
🟢 10.1.16.9	0 ms	git.corp.515support.c...	80

Ready | Display: All | Threads: 0

Nmap Scanning Techniques

Basic Scans

- Default action pings and sends TCP ACK packets to ports 80 and 443
- ARP and Neighbor Discovery (ND) sweeps on local networks

Host Discovery

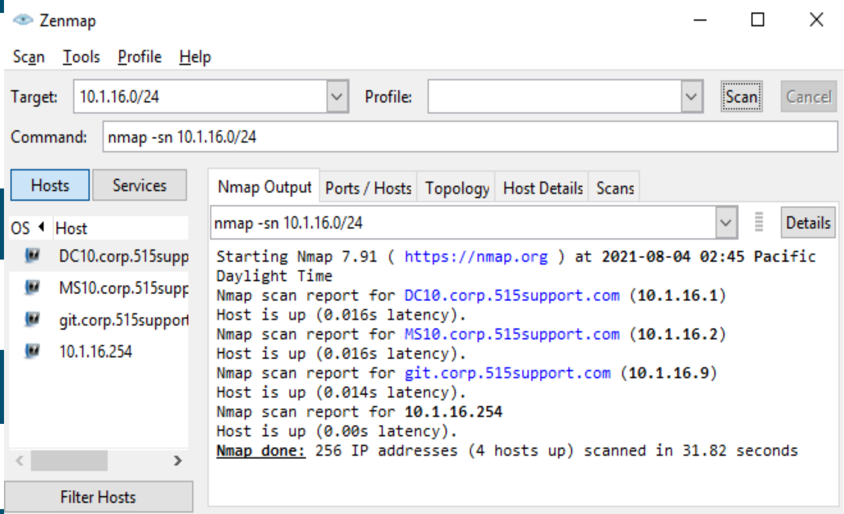
- –sn switch performs discovery without port scanning

Service and OS Detection

- Identify services and OS running on a host

Stealth Scans

- Evade detection
- Identify non-responsive hosts



Target: 10.1.16.0/24

Command: nmap -sn 10.1.16.0/24

DC10.corp.515supp
MS10.corp.515supp
git.corp.515support
10.1.16.254

```
nmap -sn 10.1.16.0/24
```

```
Starting Nmap 7.91 ( https://nmap.org ) at 2021-08-04 02:45 Pacific
Daylight Time
Nmap scan report for DC10.corp.515support.com (10.1.16.1)
Host is up (0.016s latency).
Nmap scan report for MS10.corp.515support.com (10.1.16.2)
Host is up (0.016s latency).
Nmap scan report for git.corp.515support.com (10.1.16.9)
Host is up (0.014s latency).
Nmap scan report for 10.1.16.254
Host is up (0.00s latency).
Nmap done: 256 IP addresses (4 hosts up) scanned in 31.82 seconds
```

Discovery Protocols

Cisco Discovery Protocol (CDP)

- Cisco proprietary tool
- Discovers how devices are connected in a network
- Discovers OS version and IP addresses
- Detects information from directly connected CDP devices

Link Layer Discovery Protocol (LLDP)

- IEEE standards-based protocol
- Discovers how devices are connected in a network
- Discovers OS version and IP addresses
- Detects information from all directly connected LLDP devices

Performance Monitoring

Tracks and analyzes the speed and efficiency of a network

Metrics tracking

- Bandwidth
- Throughput
- CPU and Memory
- Storage
- Latency
- Response Time
- Error Rate

Baseline establishment

- Based on historical value
- Compared to current performance

Threshold alerts

- Ensures optimal system performance
- Alerts when metrics deviate

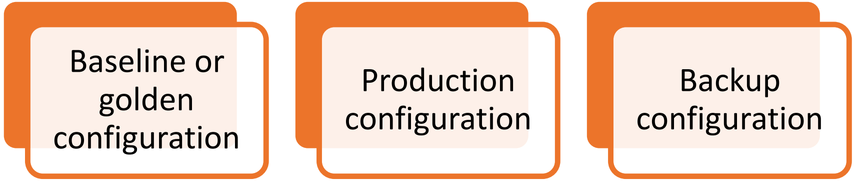
Availability Monitoring

Verifies that network devices and services are operational and accessible when needed

- Early detection of outages
- Preventing wider impact
- Optimize server performance
- Network stability
- Security threats
- External validation tools

Configuration Monitoring

- Verifies that all network appliances are in a known state



Baseline or golden configuration

Production configuration

Backup configuration

Activity: Fill in the Blank

- ____________ monitoring verifies that network
  devices and services are operational and accessible when needed.

- ____________ monitoring verifies that all network appliances are in a known state.

- ____________ monitoring tracks and analyzes
  the speed and efficiency of a network.

Poll Questions

How do network discovery tools like Nmap contribute to effective network management and security?

What are the key differences between performance monitoring and availability monitoring in network management?

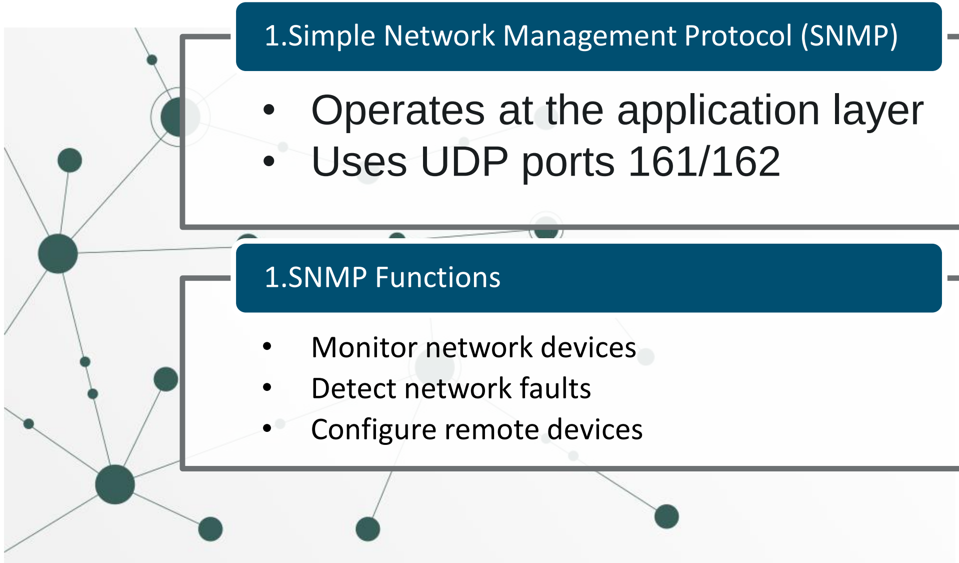
Game: "Monitor Match-Up" Match the monitoring type with its primary purpose:

1. Performance Monitoring
2. Availability Monitoring
3. Configuration Monitoring
4. Network Discovery

- A. Finds and identifies devices on the network B. Checks if network devices are working and accessible C. Tracks how well the network is running (speed, efficiency) D. Makes sure network devices are set up correctly

SNMP

Simple Network Management Protocol



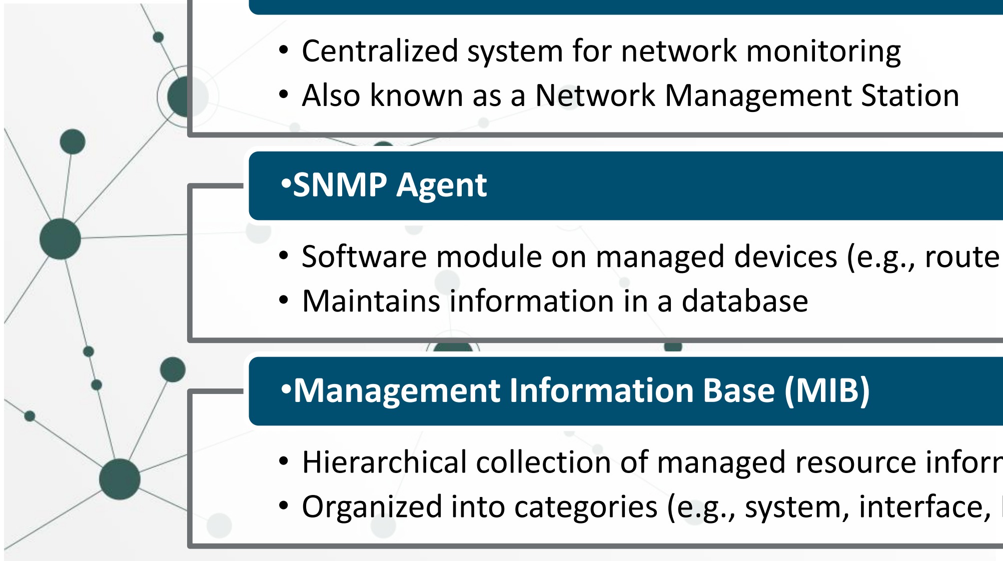
1.Simple Network Management Protocol (SNMP)

- Operates at the application layer
- Uses UDP ports 161/162

1.SNMP Functions

- Monitor network devices
- Detect network faults
- Configure remote devices

Components of SNMP



•SNMP Manager (NMS)

- Centralized system for network monitoring
- Also known as a Network Management Station

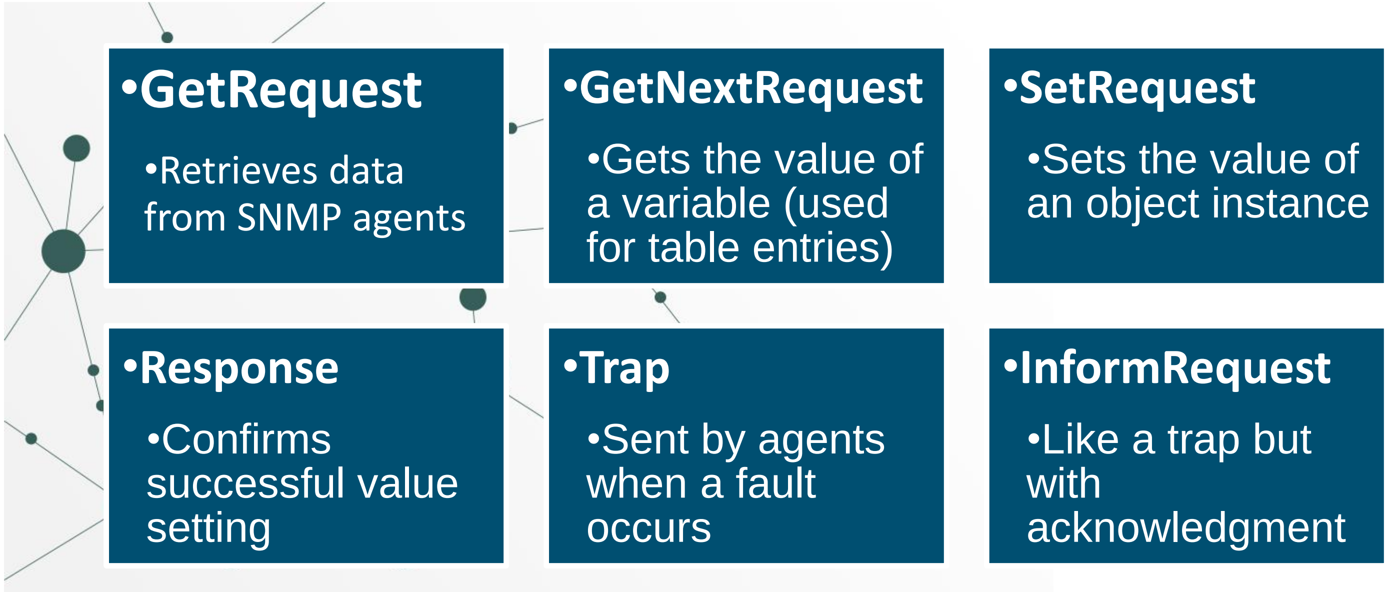
•SNMP Agent

- Software module on managed devices (e.g., routers, switches)
- Maintains information in a database

•Management Information Base (MIB)

- Hierarchical collection of managed resource information
- Organized into categories (e.g., system, interface, IP, and more)

SNMP Messages



- **GetRequest**
  - Retrieves data from SNMP agents
- **GetNextRequest**
  - Gets the value of a variable (used for table entries)
- **SetRequest**
  - Sets the value of an object instance
- **Response**
  - Confirms successful value setting
- **Trap**
  - Sent by agents when a fault occurs
- **InformRequest**
  - Like a trap but with acknowledgment

SNMP Security

•SNMP v2c Security Tips

- Avoid transmitting plaintext community strings over networks.
- Use complex community strings; avoid defaults.
- Restrict operations via access control lists to known IPs.

•SNMP v3 Advancements

- Offers encryption and strong user authentication
- Uses username lists with access permissions instead of community strings

•Auth modes

- **authNoPriv**: Authentication without encryption
- **authPriv**: Authentication with encryption using user credentials

Activity: True or False?

- An SNMP Manager is a hierarchical collection of managed resource information that is organized into categories like system, interface, IP, and more.
- **True? or False?**

EVENT MANAGEMENT

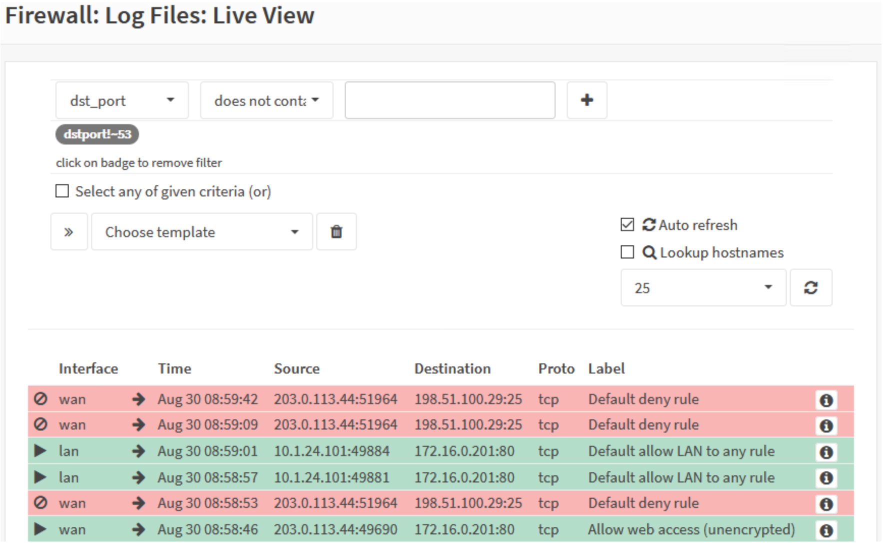
Network Device Logs

•Network Device Logs Defined

- Data sources for network monitoring, troubleshooting, security audits
- Metadata

•Key Log Types

- System Logs
- Application Logs
- Audit Logs
- Performance/ Traffic Logs



Firewall: Log Files: Live View

dst_port ▾ does not cont: ▾ +

dstport!~53

click on badge to remove filter

☐ Select any of given criteria (or)

☑ Auto refresh

☐ Lookup hostnames

25 ▾

	Interface		Time	Source	Destination	Proto	Label	
⊘	wan	→	Aug 30 08:59:42	203.0.113.44:51964	198.51.100.29:25	tcp	Default deny rule	ℹ
⊘	wan	→	Aug 30 08:59:09	203.0.113.44:51964	198.51.100.29:25	tcp	Default deny rule	ℹ
▶	lan	→	Aug 30 08:59:01	10.1.24.101:49884	172.16.0.201:80	tcp	Default allow LAN to any rule	ℹ
▶	lan	→	Aug 30 08:58:57	10.1.24.101:49881	172.16.0.201:80	tcp	Default allow LAN to any rule	ℹ
⊘	wan	→	Aug 30 08:58:53	203.0.113.44:51964	198.51.100.29:25	tcp	Default deny rule	ℹ
▶	wan	→	Aug 30 08:58:46	203.0.113.44:49690	172.16.0.201:80	tcp	Allow web access (unencrypted)	ℹ

Network Device Log Usage

•Troubleshooting & Performance

- •Pinpoint network issues
- •Optimize performance

•Security & Compliance

- •Track unauthorized access, breaches
- •Critical for security policies, regulations compliance

•Log Management Practices

- •Regular review and analysis for issue prevention
- •Secure storage for data integrity and forensic use

Log Collectors

Objective

Centralize, simplify network log management

How It Works

Aggregate log data into single repository

Benefits

Centralized Management

Efficiency

Scalability

Syslogs

Objective

Provide a standardized protocol for sending log messages

Key Features

UDP Port 514:

PRI Code

Flexibility

Advantages

Widespread adoption

Simplifies integration

Syslog Severity Levels

Code	Level	Interpretation
0	Emergency	The system is unusable (kernel panic).
1	Alert	A fault requiring immediate remediation has occurred.
2	Critical	A fault that will require immediate remediation is likely to develop.
3	Error	A nonurgent fault has developed.
4	Warning	A nonurgent fault is likely to develop.
5	Notice	A state that could potentially lead to an error condition has developed.
6	Informational	A normal but reportable event has occurred.
7	Debug	Verbose status conditions used during development and testing.

SIEM Overview

Definition

Analyzes security alerts from applications and network devices in real-time

Purpose

Integrates security information management (SIM) and security event management (SEM)

Key Functions

Log Aggregation

Event Correlation

Alerting

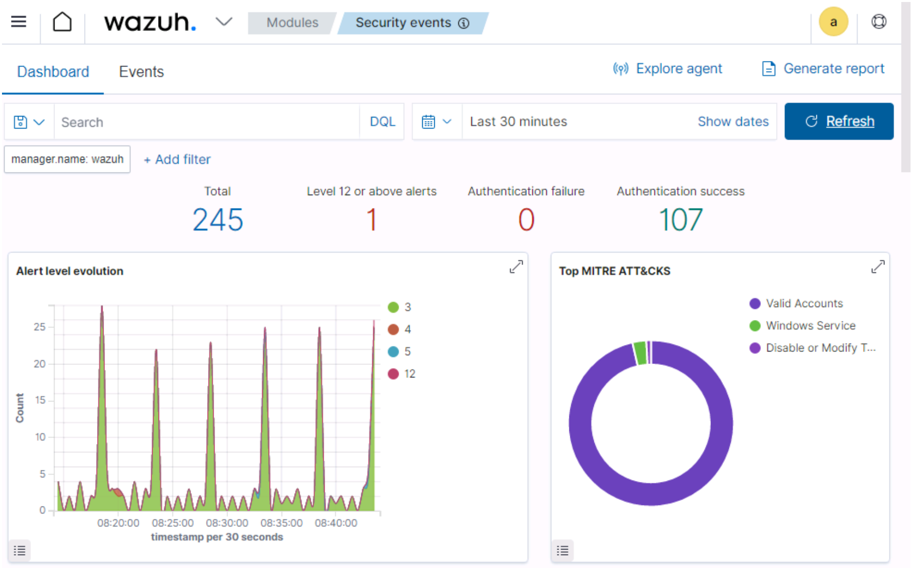
SIEM Overview

•Event Management Capabilities

- Real-time visibility
- Threat detection and response
- Compliance management

•Implementation Benefits

- Enhanced security posture
- Reduced incident response time
- Improved efficiency

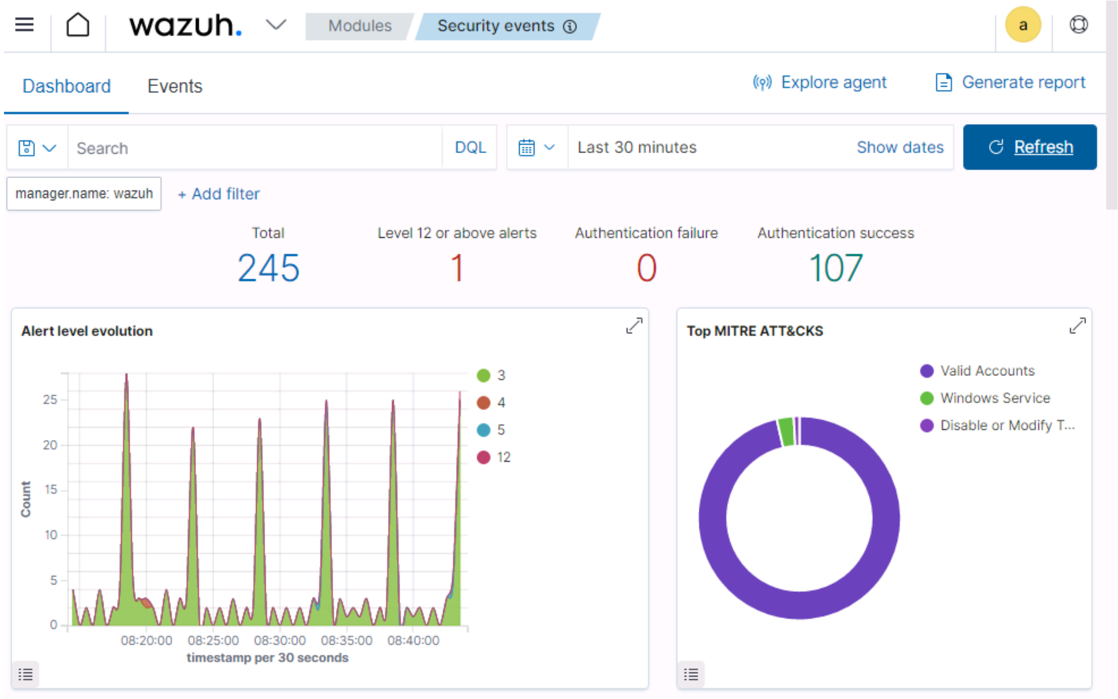


Last 30 minutes

manager.name: wazuh

Total	Level 12 or above alerts	Authentication failure	Authentication success
245	1	0	107

SIEM Example



Total	Level 12 or above alerts	Authentication failure	Authentication success
245	1	0	107

Activity: Matching

Audit Logs

Application Logs

System Logs

Performance/
Traffic Logs

•Metrics for compute, storage, network

•OS events, configuration, kernel processes

Service-specific data (DNS, HTTP)

Authentication and authorization attempts

Poll Questions

How do log collectors and syslogs contribute to effective network management and troubleshooting?

What are the key components of a SIEM system, and how does it enhance network security?

Game: "Event Management Puzzle"

- Arrange the following steps in the correct order for handling a network event:

1. Analyze event data
2. Collect logs from devices
3. Prioritize the event
4. Take appropriate action
5. Generate alert if necessary

PACKET CAPTURE & ANALYSIS

Packet Capture

Definition & Purpose

Recording network traffic for analysis and troubleshooting

Key Concepts

Use libpcap library for capturing packets

Filtering capabilities to capture specific data

Practical Application

Demonstrating how to initiate a packet capture session and important command lines (e.g., `tcpdump -i eth0`)

Packet Analysis Tools

Overview

Tools that assist in analyzing captured network packets

Used to diagnose issues or monitor network health.

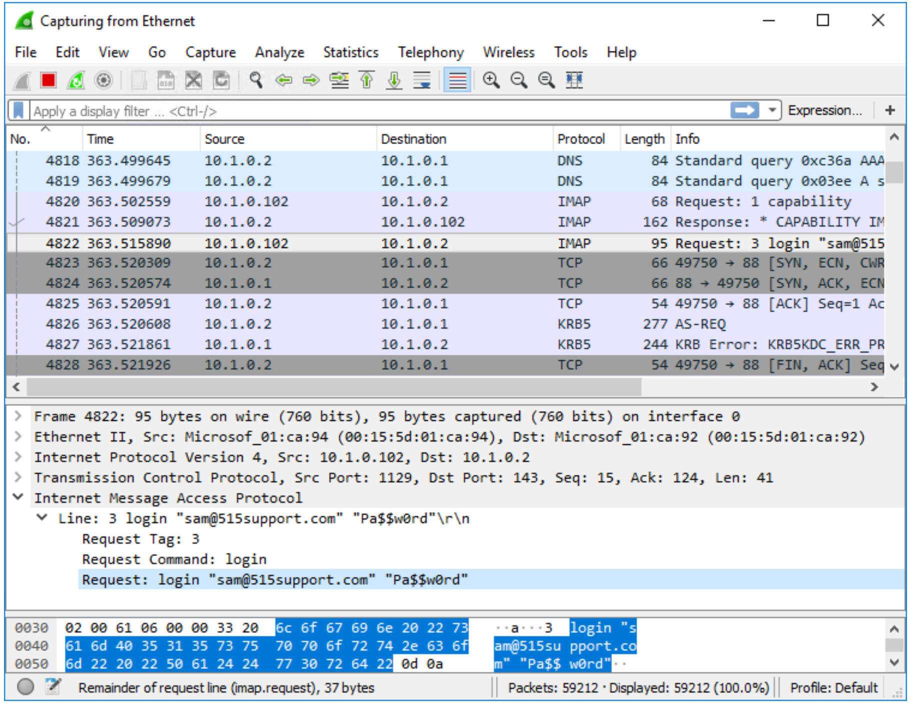
Featured Tools

tcpdump

Wireshark

ngrep

Packet Capture Analyzer Example



No.	Time	Source	Destination	Protocol	Length	Info
4818	363.499645	10.1.0.2	10.1.0.1	DNS	84	Standard query 0xc36a AAA
4819	363.499679	10.1.0.2	10.1.0.1	DNS	84	Standard query 0x03ee A s
4820	363.502559	10.1.0.102	10.1.0.2	IMAP	68	Request: 1 capability
4821	363.509073	10.1.0.2	10.1.0.102	IMAP	162	Response: * CAPABILITY IM
4822	363.515890	10.1.0.102	10.1.0.2	IMAP	95	Request: 3 login "sam@515
4823	363.520309	10.1.0.2	10.1.0.1	TCP	66	49750 → 88 [SYN, ECN, CWR
4824	363.520574	10.1.0.1	10.1.0.2	TCP	66	88 → 49750 [SYN, ACK, ECN
4825	363.520591	10.1.0.2	10.1.0.1	TCP	54	49750 → 88 [ACK] Seq=1 Ac
4826	363.520608	10.1.0.2	10.1.0.1	KRB5	277	AS-REQ
4827	363.521861	10.1.0.1	10.1.0.2	KRB5	244	KRB Error: KRB5KDC_ERR_PR
4828	363.521926	10.1.0.2	10.1.0.1	TCP	54	49750 → 88 [FIN, ACK] Seq

```
> Frame 4822: 95 bytes on wire (760 bits), 95 bytes captured (760 bits) on interface 0
> Ethernet II, Src: Microsof_01:ca:94 (00:15:5d:01:ca:94), Dst: Microsof_01:ca:92 (00:15:5d:01:ca:92)
> Internet Protocol Version 4, Src: 10.1.0.102, Dst: 10.1.0.2
> Transmission Control Protocol, Src Port: 1129, Dst Port: 143, Seq: 15, Ack: 124, Len: 41
v Internet Message Access Protocol
    v Line: 3 login "sam@515support.com" "Pa$$w0rd"\r\n
          Request Tag: 3
          Request Command: login
          Request: login "sam@515support.com" "Pa$$w0rd"
```

```
0030  02 00 61 06 00 00 33 20  6c 6f 67 69 6e 20 22 73   ··a···3  login "s
0040  61 6d 40 35 31 35 73 75  70 70 6f 72 74 2e 63 6f   am@515su pport.co
0050  6d 22 20 22 50 61 24 24  77 30 72 64 22 0d 0a      m" "Pa$$ w0rd"··
```

Remainder of request line (imap.request), 37 bytes

Packets: 59212 · Displayed: 59212 (100.0%)

Profile: Default

Capture Analysis Techniques

•Analysis Objectives

- Understanding traffic flow
- Identifying misconfigurations
- Detecting anomalies

•Wireshark Analysis Features

- Frame-by-frame header and payload examination
- Use of Follow TCP Stream to reconstruct session data

•Statistical Tools

- Conversations and Protocol Hierarchy
- Traffic analysis

Poll Questions

How does packet capture and analysis contribute to network troubleshooting and security?

What are the key components of effective traffic monitoring, and how do they help optimize network performance?

TRAFFIC MONITORING

Traffic Monitoring

Definition

Continuously observing and analyzing the flow of traffic across a network to ensure optimal performance and security

Key Points

Identifies traffic volume trends

Monitors performance to detect anomalies

Helps in capacity planning and network design adjustments

Common Performance Issues

Typical problems that affect network efficiency and user experience

•Types of Common Issues

- Packet loss, delays, and jitter affecting quality of service (QoS)
- Bandwidth bottlenecks leading to slow data transfer rates
- Misconfigured network hardware
- Outdated infrastructure

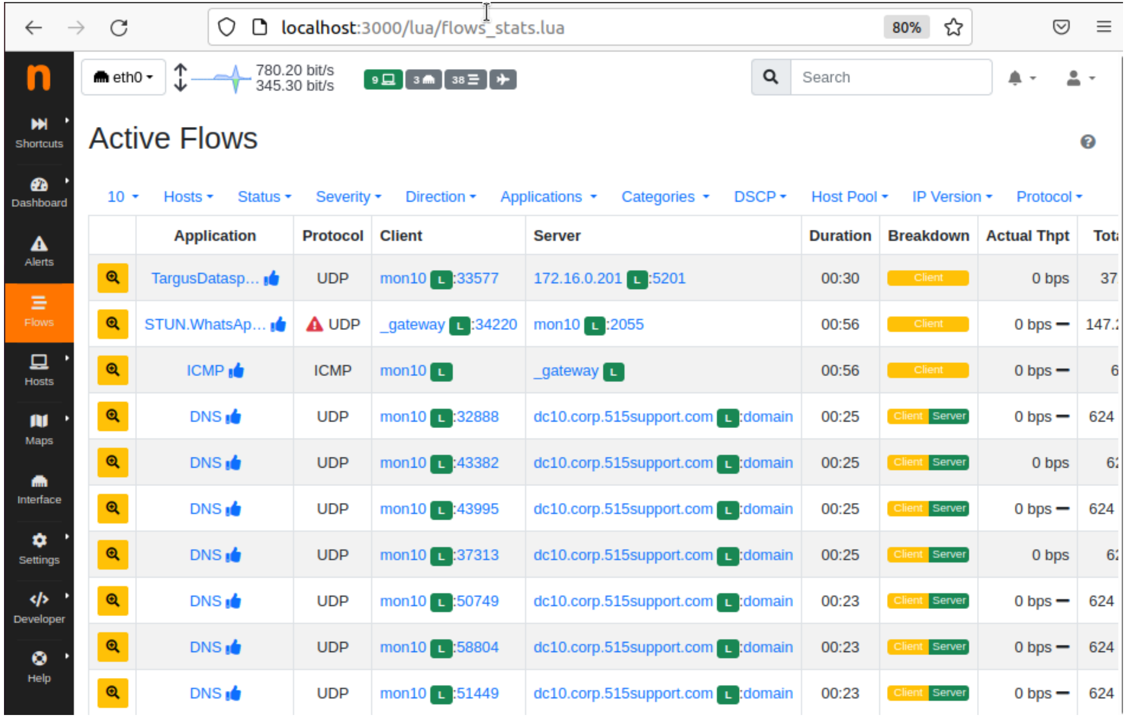
Flow Data

Information extracted from data packets that provides insights into the traffic flow within a network

•Key Points

- Includes source/destination IPs, packet sizes, and timestamps
- Essential for network performance analysis and troubleshooting
- Used in traffic profiling and anomaly detection

Monitoring Flow Data Example



Active Flows

	Application	Protocol	Client	Server	Duration	Breakdown	Actual Thpt	Tot
	TargusDatasp...	UDP	mon10 L :33577	172.16.0.201 L :5201	00:30	Client	0 bps	37
	STUN.WhatsAp...	UDP	_gateway L :34220	mon10 L :2055	00:56	Client	0 bps —	147.
	ICMP	ICMP	mon10 L	_gateway L	00:56	Client	0 bps —	6
	DNS	UDP	mon10 L :32888	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps —	624
	DNS	UDP	mon10 L :43382	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps	62
	DNS	UDP	mon10 L :43995	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps —	624
	DNS	UDP	mon10 L :37313	dc10.corp.515support.com L :domain	00:25	Client Server	0 bps	62
	DNS	UDP	mon10 L :50749	dc10.corp.515support.com L :domain	00:23	Client Server	0 bps —	624
	DNS	UDP	mon10 L :58804	dc10.corp.515support.com L :domain	00:23	Client Server	0 bps —	624
	DNS	UDP	mon10 L :51449	dc10.corp.515support.com L :domain	00:23	Client Server	0 bps —	624

Traffic Testing Tools

Definition

Applications that simulate network traffic and test the performance of network components

Key Points

Identify network bottlenecks and capacity limits

Includes packet generators, network emulators, and throughput testers

Examples: Wireshark, iperf, and NetFlow Analyzer

Bandwidth Management

Definition

Techniques to control traffic flow in a network to optimize or guarantee performance

Key Points

Allocates bandwidth so essential services have priority

Prevents network congestion and ensures fair usage

Methods: Rate limiting and traffic policing

Traffic Shaping

Definition

Prioritizing network traffic to ensure critical
applications receive their required bandwidth

Key Points

Delaying packets to regulate traffic flow and reduce congestion

Tools for traffic management: QoS, DiffServ, and MPLS

Ensures high priority services maintain performance

Activity: Two Truths and a Lie

Bandwidth bottlenecks lead to slow data transfer rates.

Bandwidth management is used to control traffic flow in a network to optimize or guarantee performance.

Bandwidth management tools include QoS, DiffServ, and MPLS.

Game: "Traffic Tools Matchup"

- Match the tool or technique with its primary use:

1. Packet Capture
2. Flow Data Analysis
3. Traffic Shaping
4. Bandwidth Management

- A. Controls overall network traffic flow B. Records individual data packets for detailed examination C. Prioritizes certain types of network traffic D. Provides overview of traffic patterns and trends

Summary

- Implement configuration and change management practices
- Maintain a detailed network asset inventory with diagrams
- Deploy network analyzers for performance and activity insights
- Configure endpoints for log collection
- Define metrics to monitor network health, traffic, and device performance

Discussion time: Please type your questions in chat

- Questions over content.
- Share you experience.
- What would you like to see different moving forward?

Let’s keep the conversation going in the CompTIA Instructor Forum: https://cin.comptia.org